

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri

FILED

OCT 13 2015

U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST. LOUIS

In the Matter of the Search of

3245 Quervo Ln.
Imperial, MO 63052 Eastern District of Missouri
and all computers, computer hardware, computer and digital
media, and wireless telephones therein.

Case No. 4:15 MJ 262 DDN

APPLICATION FOR A SEARCH WARRANT

I, Michael Spreck, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

3245 Quervo Ln. Imperial, MO 63052 Eastern District of Missouri and all computers, computer hardware, computer and digital media, and wireless telephones therein.

located in the EASTERN District of MISSOURI, there is now concealed

SEE ATTACHMENTS A and B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18:2251
18:2252 and 18:2252A

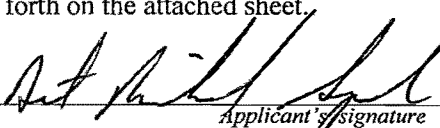
Offense Description

Production of Child Pornography
Possession, Receipt, Distribution and Transmission of Child Pornography

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE


- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


 Applicant's signature
 Special Federal Officer Michael Spreck
 Federal Bureau of Investigation
 Printed name and title

Sworn to before me and signed in my presence.

Date: October 13, 2015

City and state: St. Louis, MO


 Judge's signature
Honorable David D. Noce, U.S. Magistrate Judge
Printed name and title

AUSA: Robert F. Livergood, #35432MO

IN THE UNITED STATES DISTRICT COURT FOR THE
DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH)
OF:)

UNDER SEAL

3245 Quervo Ln.)
Imperial, MO 63052)
Eastern District of Missouri)
and all computers,)
computer hardware,)
computer and digital media, and)
wireless telephones therein.)

Case No. 4:15 MJ 262 DDN

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

INTRODUCTION

I, Michael Spreck, having been first duly sworn, do hereby depose and state as follows:

1. I am a Detective with the St. Louis Metropolitan Police Department and am currently assigned as a Special Federal Officer (SFO) with the Federal Bureau of Investigation (FBI). I have been employed by the St. Louis Metropolitan Police Department for nineteen years, and am assigned to the Major Fraud/Cyber Crime Unit, Crimes Against Property Division, in the Bureau of Criminal Investigation and Support. Since November 2009, I have been assigned to the FBI St. Louis Division. I investigate computer crimes which includes cases involving the sexual exploitation of minors. During my career as a detective, I have conducted numerous investigations regarding the sexual exploitation of children that involve the use of a computer. The use of a computer in these cases were violations of Title 18, United States Code, Sections 2251, 2252, and 2252A, which criminalize the production, possession, receipt, distribution and transmission of child pornography. I have been personally involved in the execution of search warrants to search residences and seize material relating to the sexual

exploitation of minors. This material has included computers, computer equipment, software, and electronically stored information. During the course of my career, I have had contacts and dealings with informants, other police officers, and subjects known to possess, distribute and manufacture child pornographic images.

2. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18 of the United States Code. That is, I am a Special Federal Officer (SFO) with the Federal Bureau of Investigation who is empowered by law to conduct investigations of, and make arrests for, offenses including those enumerated in Title 18, United States Code, Sections 2251, 2252, 2252A, 2422 and 2423, *et seq.*

3. This affidavit is made in support of an application for a warrant to search the following location, referred to as the "TARGET LOCATION":

a) 3245 Quervo Ln., Imperial, MO 63052

4. The TARGET LOCATION described in Paragraph 37 and in Attachment A is to be searched for evidence of violations of Title 18, United States Code, Section 2251(a) and (e) (production of and conspiracy to produce child pornography); Title 18, United States Code, § 2252A(a)(2) (receipt and distribution of child pornography); Title 18, United States Code, § 2422 (coercion and enticement); and Title 18, United States Code, Section 2252A(a)(5)(B) (possession of child pornography), (collectively, the "SPECIFIED FEDERAL OFFENSES").

5. The statements in this affidavit are based in part on information and reports provided by FBI Special Agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents; information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by federal agents; independent investigation and analysis by FBI agents/analysts and

computer forensic professionals; and my experience, training and background as a law enforcement officer. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violations of the above-referenced statutes are located at/within the TARGET LOCATION.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

6. Through my experience and training, and that of other law enforcement officers, the following traits and characteristics are generally found to exist and be true in cases involving individuals who collect child pornography:

a. The majority of individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

b. The majority of individuals who collect child pornography often seek out likeminded individuals, either in person or on the internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact also helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different internet based vehicles used by such individuals to communicate with each other include, but are not limited to, websites, email, email groups, bulletin boards, internet chat programs, newsgroups, instant messaging, and other similar vehicles.

c. The majority of individuals who collect child pornography often collect, read, copy or maintain names, addresses (including email addresses), phone numbers, or lists of

persons who have advertised or otherwise made known in publications and on the internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

d. The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect their collections from discovery, theft, and damage. Your Affiant knows from training and experience that such individuals have been known to maintain possession of their child pornography for years, or even decades. They almost always maintain their collections in the privacy and security of their homes or other secure locations.

7. Your affiant believes the subject of the instant investigation to be a collector of child pornography because, as further described herein, the subject has participated in a criminal scheme to entice minors to produce child pornography images, communicated with other like-minded individuals about such a scheme, and taken significant steps to conceal his location and identity from others.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

8. As described above and in Attachment B, this application seeks permission to search for evidence of violations of the SPECIFIED FEDERAL OFFENSES that might be found in the TARGET LOCATION, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

9. *Probable cause.* I submit that if a computer or storage medium is found in the TARGET LOCATION, there is probable cause to believe evidence of violations of the SPECIFIED FEDERAL OFFENSES will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the internet are sometimes automatically downloaded into a temporary internet directory or “cache.”

10. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the TARGET LOCATION because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element, or alternatively, to exclude the innocent from further suspicion. In my training and

experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user’s

state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to access, receive, and distribute child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is

an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of internet discussions about the crime; and other records that indicate the nature of the offense.

11. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises is not feasible. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or

months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

12. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

PROBABLE CAUSE

13. On January 22, 2015, the FBI arrested a subject (hereinafter "S1") on charges related to his use of a website that facilitated the sexual abuse of minors and the production and trafficking of child pornography. Following his arrest, S1 consented to being interviewed by

law enforcement agents. During the interview, S1 admitted to accessing, using, and sharing child pornography to that website. S1 also alerted agents to the existence of another website used by individuals to help facilitate the enticement of minors to engage in sexually explicit conduct via web camera (this website is known to law enforcement and has been identified. It will hereinafter be referred to as "WEBSITE A"). S1 told investigators that he was a member of WEBSITE A.

14. S1 subsequently consented to allow the FBI to assume his online identity on the site. Between the dates of January 26, 2015 and March 11, 2015, an Under Cover Law Enforcement Officer (UCA) logged into WEBSITE A on various dates and times and was able to observe the activities of members of WEBSITE A. When going to the site, the UCA had to log in using a specific name and password. Once logged in, the UCA observed that the site's main page functioned as a chat room. The right side of the page listed the members who were logged into the site at the time and the main page was a continuously running chat. In the chat section, the UCA observed that the users posted links in the forum to publicly available websites where children used live webcams, such as, but not limited to: Kik, YouNow (YN), YouTube, Chateen (CT), Condorchat (CC), and mylol.¹

15. At the bottom of the homepage of WEBSITE A, there were several tabs that appeared to represent different "tools" the members could use to target specific people chatting on YouNow. One of the tabs labeled "Vault" appeared to be a listing of files stored on www.mega.co.nz, a free cloud storage site that offers encryption, with the encryption key only

¹ Kik is an instant messaging application for mobile devices that also allows users to share photos and videos. YouNow is a social networking site offering live streaming broadcasting capabilities. YouTube is a video-sharing website. Chateen and Condorchat are social networking sites utilizing live video and audio chat. Mylol is a teen dating site for teens in the US, Australia and the United Kingdom.

known to the up-loader, not to the site administrators. The UCA noted that several of the files available in the Vault appeared to be child pornography.

16. One of the files the UCA viewed in the Vault appeared to be a composite of images from a video file that depicted a prepubescent girl exposing her vagina and spreading her labia as a close up to the camera.

17. Another file viewed by the UCA in the Vault appeared to be a composite of images from a video file depicting a nude pubescent girl exposing her breasts and vagina and masturbating.

18. On February 27, 2015, the UCA logged into the site and attempted to access the Vault but received the following error message: "Sorry! Your access to the Vault has been revoked until you have a discussion with our entire team in our chat. Inactives do not deserve access to the Vault. Thanks for your understanding and hope to see you soon to discuss this issue!" On March 11, 2015 the UCA was logged into the site when the administrator told the UCA that the UCA's access had been revoked due to the UCA continuing to attempt to access the Vault without contributing material to the site.

19. Open source searches revealed the IP address of the website to be hosted by OVH, a company located in Montreal, Quebec, Canada. On March 5, 2015, pursuant to a Mutual Legal Assistance request, members of the Royal Canadian Mounted Police (RCMP) provided the FBI with registration information for WEBSITE A. On March 11, 2015, the site was seized and taken down by the RCMP. An image of the server that hosted WEBSITE A was obtained by the RCMP and later provided to the FBI. A review of the image revealed various archive files and log files related to WEBSITE A, including but not limited to user login records

and user chat records. OVH records provided the identifying information of the site administrator, (hereinafter "S2").

20. On April 15, 2015, the FBI executed a search warrant at the residence of S2. S2 consented to being interviewed by FBI agents. During the interview, S2 admitted to using WEBSITE A to facilitate the SPECIFIED FEDERAL OFFENSES. S2 stated that WEBSITE A originally consisted of approximately 10-20 members, approximately 10 of which were still very active members. Members of the site were the people from other groups on the internet that were the most motivated to go out and get child pornography. S2 described WEBSITE A as a text chat room where members would talk about getting children to self produce images or videos of themselves engaged in sexually explicit conduct on social media via webcams, as explained in more detail in paragraph 22.

21. Upon reviewing the site and the UCA recordings of the site, law enforcement officers were able to determine several ways the members targeted and coerced children into self producing images or videos of sexually explicit conduct. S2 confirmed that different members of the site had different rolls and/or techniques they each "specialized" in for the group. Such rolls and/or techniques are as follows:

- a. Chatter: a member who would actually chat with children in social media, usually in a text-chat format, but sometimes using voice calling or text messaging.
- b. Looping, also known as (aka) lewping: a term used to describe the process of pretending to be a minor child by showing a previously recorded webcam video and playing it as if it were a live-feed video. Members used this method to "prove" to minor children that they were also children. The method was used

sparingly due to the chance the real minor child may request the member to conduct a specific action (like waving).

- c. Linking: a member whose role was to find potential minor children engaging in, or willing to engage in sexually explicit conduct, and linking the minor child's direct social media account information to the group. Often, linking also involved finding the child on multiple social media accounts, so the minor child could be contacted in multiple locations. Having multiple locations to contact the children was important to the members in case the child were to get kicked off a site for engaging in sexually explicit conduct. Many social media account services monitor, or have a reporting system, where users can report inappropriate conduct of other users.

22. Members of the site also used their own terms to describe their actions, as well as the children they were targeting. Examples of that specialized language include:

- a. Bating/Bate: Short for masturbating/masturbate
- b. Win: a term used to describe a video where the member was able to get the minor child to engage in sexually explicit activity, such as "bating"
- c. Catfish: a term used to describe pretending to be someone you are not on the internet by creating false profiles. Members of this group that participated in chatting and looping would create profiles pretending to be minor children of the same age of the minor children they were targeting
- d. Maxclock or Max Clock: A plus and minus system to describe the age of the minor children they were targeting, based off the 12 hours of the clock. For

example, Maxclock +2 would make the child 14 years old. Maxclock -2 would make the child 10 years old

- e. IRL: In Real Life
- f. Banned: when a user of a social media account is kicked off the service for engaging in some conduct that was against the site's rules, often sexually explicit activity
- g. Pedro: a pedophile
- h. Upping/Upped: to upload to the Vault (explained further in paragraph 25e)

23. The site had links and special tools designed by members to assist in finding children to engage in sexually explicit conduct for the purpose of producing images and videos of that conduct.

24. Examples of the tools, as described by S2 included:

- a. Snapscan: YouNow offers users the ability to create still frame images of live broadcasts called "snapshots." The Snapscan tool was created by members of WEBSITE A to pull all the snapshots off YouNow servers, allowing WEBSITE A users to more efficiently determine whether a particular YouNow user was underage and likely to engage in sexually explicit activity.
- b. Pedroscan: a tool that allows members of WEBSITE A to put in the YouNow user name of any other like-minded individual ("pedros") and the tool will then show all the children that individual has "liked" or "fanned"² previously.
- c. Mass Viewer (YNMV): a tool that allows members of WEBSITE A to add multiple filters, to include Number of Cams, Tags, Stars, and Location. After

² "Fanning" is the ability to have one user click a button to show another user that they are a "fan" of their broadcasts. The more fans a user has, the more status is given to them within the site.

adding the filters, the tool shows all live broadcasts on YouNow that fit those criteria.

- d. Requests: members were able to put in requests for other members to target a specific child and later share the recording of the broadcast with them.
- e. Vault: a listing of encrypted compressed files stored on www.mega.co.nz. All members of WEBSITE A used the same password to encrypt the files and would share the recording of the videos they were able to find and/or produce. All members of WEBSITE A that contributed to the site were given the password to the Vault files. Nearly all files in the Vault contained child pornography.

25. A few days after WEBSITE A was taken down by the RCMP, S2 put the same site back up on a different IP address (hereinafter referred to as WEBSITE B), hosted by a company based out of the United Kingdom.

26. S2 provided the FBI with root access to the site and the FBI shut down the site on April 23, 2015. Prior to the shutdown, a review of the site revealed various archive files and log files related to WEBSITE B, including but not limited to user login records and user chat records.

IDENTIFICATION OF SUSPECT AND TARGET LOCATIONS

27. On March 11, 2015, pursuant to a mutual legal assistance treaty request, the RCMP provided federal law enforcement officers with an image of the server seized from the OVH server hosting WEBSITE A. A review of those log files revealed IP address records, chat message records and login records. Amongst the various records, within the log files from this server, your affiant located IP address 24.171.8.129 for user "Terp." Chat messages associated with these records were indicative of enticing children. The user Terp engaged in chat

messages that included linking to outside social media accounts of girls, discussion of what he was able to get the girls to do on those accounts, and using the above mentioned tools offered on the site.

28. User Terp was observed to have been logged into WEBSITE A on several occasions between July 22, 2014 and August 21, 2014. Terp was involved in uploading files to the Vault, linking, and chatting.

29. On or about August 1, 2014, user Terp was viewed on WEBSITE A communicating with other site members. Terp posted the following:

Terp: i upped [victim name redacted] in case anyone missed it earlier
Terp: small wins

30. In the above communication, Terp was telling the other members he had just uploaded a file to the Vault that included getting the child to engage in sexually explicit behavior.

31. On or about August 5, 2014, user Terp was viewed on WEBSITE A communicating with other site members. Terp engaged in a conversation with another WEBSITE A user (hereinafter referred to as S20) and had the following conversation:

S20: "Snapchat- [NAME REDACTED] Instagram- [NAME REDACTED] twitter- [NAME REDACTED] kik- [NAME REDACTED] New York. 13. 9th grade. - Whitesboro, New York"
[...]
Terp: can someone upload [NAME REDACTED] befoare it wont play for me
S20: the fuck, yn banned her
S20: I'm downloading the last beast, but userId":3931521
[http://www.younow.com/\[NAME REDACTED\]/15092321/0/0/b/August-4,-2014](http://www.younow.com/[NAME REDACTED]/15092321/0/0/b/August-4,-2014)
should be also interesting
S20: ill upload the vid

32. On or about August 6, 2014, user Terp was viewed on WEBSITE A communicating with other site members. Terp engaged in a conversation with two other WEBSITE A users (hereinafter referred to as S20 and S37) and had the following conversation:

S37: [http://www.younow.com/\[name redacted\]](http://www.younow.com/[name redacted])
Terp: nice find
S20: wow
Terp: logging in now to get her nakeder
[...]
Terp: not many people in there that is good
Terp: make it happen people
S20: it would be a win on stickam, but we don't have the time :(
[...]
Terp: i got her to show boobs and ass score 1 for me
[...]
Terp: got her to flash again
Terp: my god i didnt think she would keep going i told her i was going to bed
Terp: if i didnt do that i might have got pussy by now
S20: no
Terp: someone ask her for puss
S20: i did
Terp: what did she say
Terp: im gonna try to get some win on kik anyways she told me to text her on kik

33. In the above communication, S37 posted a link to a live feed broadcast of a child on YouNow. Terp said there were not many people watching the broadcast, so it would be easier to convince the girl to engage in sexually explicit conduct. Later, Terp said he was chatting with her and got her to show her breasts and buttocks. He said the child gave him her kik account and he planned to get her to show her vagina by using the kik account.

34. IP address 24.171.8.129 is controlled by Charter Communications. Law enforcement sent an administrative subpoena to Charter for information concerning the location of the digital device that used the IP address 24.171.8.129 between 7/22/2014 9:39:00 PM and 8/21/2014 7:33:37 PM. Documents provided in response to that subpoena indicated that this IP

address was assigned to Charter Communications and subscribed to by Bryan Cripe at 3245 Quervo Ln., Imperial, MO 63052.

35. On October 5, 2015, I reviewed the Missouri Department of Motor Vehicles (DMV) database using queries for BRYAN CRIPE. The results yielded information regarding an individual named BRYAN LEE CRIPE who is currently residing at the TARGET LOCATION.

36. On October 5, 2015 a representative of Ameren UE was contacted and indicated that service is being provided to BRYAN CRIPE at the TARGET LOCATION since December 5, 2003 until present.

37. On October 5, 2015, surveillance of the TARGET LOCATION to be searched, as described in Attachment A, revealed that it is a two story wood structure residence having the numerical address of 3245 Quervo Ln., displayed above the entrance door. The residence is located on the north side of the street with the entrance facing south. The above listed residence is located in the Eastern District of Missouri.

38. On October 5, 2015, Affiant observed a 2009 Chevy bearing Missouri license plate DB7-Z1V parked in the garage of the TARGET LOCATION. Affiant also observed a white male operating a 2004 GMC truck bearing Missouri license plate 1WA-320 pull into the driveway of the TARGET LOCATION and enter the TARGET LOCATION via the garage. The white male exiting the GMC truck had similar facial and physical features of BRYAN CRIPE'S Department of Motor Vehicle picture. A computer check of the Missouri Department of Revenue revealed the 2009 Chevy having license plate DB7-Z1V and the 2004 GMC truck having license plate 1WA-320 to be registered to a BRYAN CRIPE and KRISTY CRIPE at the

TARGET LOCATION.

39. A search of TLO information database (a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, etc.) was conducted for the TARGET LOCATION. These public records indicated that BRYAN CRIPE's current address is 3245 Quervo Ln., Imperial, MO 63052.

40. A computer inquiry of Jefferson County Assessor's Office revealed the TARGET LOCATION to be registered to a BRYAN L CRIPE and KRISTY E CRIPE.

41. On October 6, 2015, I received information from the United States Postal Service's ("USPS") that BRYAN CRIPE is receiving mail at 3245 Quervo Ln., Imperial, MO 63052.

42. Based upon your affiant's training and experience, your affiant believes that the user of IP address 24.171.8.129 was a member of WEBSITE A and conducted activity involving the enticement of children on those websites. Your affiant further believes the user of IP address 24.171.8.129 resides at the TARGET LOCATION, which contains instrumentalities of and/or evidence related to violations of Title 18, United States Code, Sections 2251, 2252A(a)(2), and 2252A(a)(5)(B), and 2422.

CONCLUSION

43. Based upon the information above, your Affiant respectfully submits that there is probable cause to believe that the Specialized Federal Offenses have been violated and that there is probable cause to believe that evidence of violations of the Specialized Federal Offenses can be found in the TARGET LOCATION. WHEREFORE, your Affiant respectfully requests that the Court issue a search warrant for the items listed in Attachment A of this affidavit, which are incorporated by reference as if fully set forth herein.

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

3245 Quervo Ln., Imperial, MO 63052

3245 Quervo Ln., Imperial, MO 63052 is a two story wood structure residence having the numerical address of 3245 Quervo Ln., displayed above the entrance door. The residence is located on the north side of the street with the entrance facing south.



ATTACHMENT B

PROPERTY TO BE SEIZED AND SEARCHED

1. All records relating to violations of Title 18, United States Code, Sections 2251, 2252A(a)(2), and 2252A(a)(5)(B), and 2422 which may be found at the TARGET LOCATION more fully described in Attachments A:

a. Any and all notes, documents, records, or correspondence pertaining to violations of 18 U.S.C. §§ 2251, 2252A and 2422, or to child pornography as defined under Title 18, U.S.C. § 2256(8).

b. Any and all correspondence identifying persons transmitting, receiving or possessing, through interstate commerce including by U.S. Mails or by computer, any visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, U.S.C. § 2256(2).

c. Any and all records, documents, invoices and materials that concern any accounts with YouTube, You Now, Chat Teen, Comcast or any other Internet Service Provider, screen names, or email accounts.

d. Any and all visual depictions of minors, to include depictions of minors engaged in sexually explicit conduct, nude pictures, and modeling.

e. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records pertaining to the preparation, purchase, and acquisition of names or lists of names.

f. Any and all documents, records, or correspondence pertaining to occupancy or other connection to 3245 Quervo Ln., Imperial, MO 63052.

h. Any and all diaries, notebooks, notes, pictures, emails, chats, directions, maps, banking, travel, documents, and any other records reflecting personal contact and any other activities with minors.

i. Any and all notes, documents, records, photos or correspondence that indicate a sexual interest in children, including, but not limited to:

- i. Correspondence with children;
- ii. Any and all visual depictions of minors;
- iii. Internet browsing history;
- iv. Books, logs, emails, chats, diaries and other documents.

2. Any and all web cameras, video cameras, videotapes, cameras, film, cell phones with cameras and/or internet capability, or other photographic equipment that are instrumentalities of and/or contain evidence related to violations of Title 18, United States Code, Sections 2251, 2252A(a)(2), and 2252A(a)(5)(B), and 2422.

3. Computers or storage media used as a means to commit the violations described above, including producing, possessing, receiving, and distributing child pornography, and coercion and enticement, in violation of Title 18, United States Code, Sections 2251, 2252A(a)(2), and 2252A(a)(5)(B), and 2422.

4. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing

history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web

- pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.
5. Routers, modems, and network equipment used to connect computers to the internet.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, personal data assistants, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.